Fox Rothschild Podcast

The Presumption of Innocence

Episode 48: Digital Boundaries: Fourth Amendment Protections in a Connected World

Featuring Matt Adams of Fox Rothschild and Michael Price of the NACDL's Fourth Amendment Center

Adams: Hi, everyone, and welcome back to "The Presumption of Innocence," a podcast brought to you by the White-Collar Criminal Defense and Regulatory Compliance practice at Fox Rothschild.

I gotta say, the National Association of Criminal Defense Lawyers, or NACDL is a, an organization near and dear to my heart. I'm a proud card-carrying member of the NACDL. I am a past president of the New Jersey chapter, the local chapter of the NACDL. And today I have the great fortune of being joined by Michael Price. Michael Price is with the NACDL's Fourth Amendment Center, which offers direct assistance to defense lawyers handling cases involving new surveillance tools, technologies and tactics that infringe on the constitutional rights of people in the United States of America.

This center is available to help members of the defense bar bringing new Fourth Amendment challenges. I've been on the front lines with them and they are the absolute best when it comes to the intersection of the law and technology. And Mike is just a fantastic and well-informed guy when it comes to all this.

Mike, welcome to the program today. It's so great to have you.

Michael Price: Thank you, Matt. Real pleasure to be with you.

Matt Adams: I've given a little bit of a plug to the Fourth Amendment Center at NACDL, but in your words, what do you do on a daily basis? Just so our audience knows what's going on behind the scenes at this wonderful organization. And in particular, the mission of your group, which is really focused in on all of these technologies that have become a part of our regular lives in America in 2024, but at the same time, present unique challenges that may not have existed or may have existed with their bricks-and-mortar counterparts in another time. So talk a little bit about the mission of the Fourth Amendment Center.

Michael Price: Well, the Fourth Amendment Center is fantastic. We've been around for about six years now. And we provide resources and trainings for the defense bar on Fourth Amendment issues involving new technologies. And we also provide direct litigation assistance. If you get one of these issues in your case, you can give us a call. You don't have to be an NACDL member to get this assistance. It is a terrific organization and you should join, but anybody can call up and get some

help with their case, whether it's just talking an issue through, or, you know, sometimes we get heavily involved and we'll actually come in and help litigate the case.

Matt Adams: Yeah, and you're the litigation director, if I'm not mistaken. Correct, right?

Michael Price: That's correct, I'm the litigation director.

Matt Adams: And you guys are in the trenches with defense lawyers representing their clients, often as amicus, and sometimes in more direct ways even. And I know you know you and I were together on some novel issues that came before the New Jersey Supreme Court back in the *Andrews* case.

We had the great fortune of being side by side in arguing that matter. Unfortunately, cert was denied at the United States Supreme Court, but that issue is still lurking around as it relates to the compulsion to decrypt mobile devices.

And I've got a wish list of things I want to talk to you about today, because I think they are the hot-button topics in Fourth Amendment law as it relates to this intersection of the law and technology.

So, let's start with geofencing. Quickly, what is a geofence? We've heard a lot about this in the most recent court terms that have rolled out. And we have a pretty hot debate going on right now in this country about geofencing. And I'm fully aware of the fact that you can't comment on certain direct cases because you're that much in it that you're in those cases, and not able to comment specifically on the facts of those cases. But tell us, for our audience, what a geofence is, if our audience members want to be informed on that hot-button technology.

Michael Price: It's pretty scary. It's like, what I say is it's what happens when Google searches for you. And, uh, it's part of, we call these reverse warrants. But think of a normal warrant: naming a suspect and establishing probable cause to search their cell phone location data. And now imagine that process in reverse. The police don't have a suspect, right, they don't have probable cause to search anyone in particular.

So they get a warrant to search everyone who was near the scene of the crime and come up with a suspect later. That is a geofence warrant. It is an epic dragnet. It requires Google to search hundreds of millions of users' accounts for something called location history data.

Matt Adams: Let me get this straight. I'm sitting in my office right now, okay. There's about eight banks within a five-block radius that I could walk to any one of them right now. Let's assume one of those banks gets robbed. You're telling me that I'm sitting in my office talking with you and because I'm within this short, few-block radius of these banks as they get robbed, it's possible that one of these geofence warrants would pick up my data.

Michael Price: Right, yeah. Google doesn't know who was where ahead of time. They have to, at the government's direction, search the location history of every single person that has that thing enabled. That's hundreds of millions of people. And then they provide the results. You know,

everybody who showed up in that circle, say, around that bank, they provide that information to law enforcement.

So, yes, if you have location history on your phone, your data is getting searched.

Matt Adams: Based on your experience, how does law enforcement use that data? Because it strikes me that it's so wrought with potential pitfalls that here you are with this massive quantity of data, you've got to apply some level of search criteria to make it useful, right? So, where do you start? Do you start with people that have criminal histories? Do you start with people that look a certain way? Do you start with people that... you know, I don't know, where do you start? From your experience, how is that data even useful? Or what's the argument that that data is even useful.

Michael Price: You know, I think this is a really important point because there isn't a whole lot of direction for how police are supposed to use this data once they get it. And it's part of the problem with these warrants. It's really, you know, up to law enforcement and Google to sort of work it out. And a judge is not really a part of that process.

So, you know, law enforcement will plot these coordinates on a map. And they'll try and look for devices that fit the timeline of the crime. So, you know, device that, you know, showed up shortly before the bank got robbed and left right after, something along those lines.

But it really is a fishing expedition. Law enforcement doesn't know what they're going to get until they get it and they put it on a map and they take a look at it. And what they can do... and this is sort of, you know, the second part of these geofence warrants is that they, they identify what they call "devices of interest." How they do that is anyone's guess. And then they can go back to Google and get additional information about where those devices came from and where they went to, uh, so all without the confines of the geofence.

You can literally see people driving from their homes to the bank and dropping their kids off at school.

Matt Adams: The Fourth Amendment, a byproduct of the Constitution, which is, I don't know, a couple of centuries old at this point. Could it ever have envisioned this technology happening in 2024 where we are that connected that we can reverse engineer someone's location like this? Because to me, it's antithetical to that freedom to be free from warrantless searches and seizures. I guess proponents of the use of this might say, Okay, well, you choose to use your device, this cell phone that you could, you know, do basically anything with in this day and age, you choose to carry it with you. So, you're almost consenting to a decreased expectation of privacy because you decide to comport yourself with modern customs?

I mean, isn't that a stretch of logic?

Michael Price: We certainly argue, first of all, that you have a privacy interest in your location. That it's your data, just like your email, your documents, your photos, it's your location. And, the Supreme Court in *Carpenter* in 2018 held that regular cell site location information was private, at least for

seven days or more. And so our argument here is that it is as private, if not more so, than the cell site data in *Carpenter*. And that searching everybody without probable cause for anybody is a general warrant, an unconstitutional general warrant. You have no probable cause to search any person's account and you are not identifying whose account you're going to search before you go and search them. So, it is this open-ended sort of invitation to go rummaging through people's data in search of a suspect. That is, I think what the Fourth Amendment was designed to prevent.

And to your point, you know, I think that the technology here is, you know, on a level that I don't think the framers could have imagined. But they certainly were aware of this general warrant problem and wrote the Fourth Amendment to put a stop to that, right. So, you know, I think... and we're certainly seeing some courts now recognize that. The 5th Circuit in particular held that they are, in fact, unconstitutional, general warrants. And actually, there's a case out of Eastern Oklahoma, the Federal District for Eastern Oklahoma, decided just this week, finding, again, finding a geofence warrant unconstitutional. Finding no good faith. So I think some courts are recognizing now the inherently problematic nature of geofence warrants.

Matt Adams: And I know you can't speak to the specific facts of any particular case, but is this poised for a showdown at the Supreme Court?

Michael Price: Well, right now there, there is a fairly cavernous circuit split between the 4th and 5th Circuits, uh, with the Fourth Circuit finding that location data isn't private at all and the 5th Circuit finding that these are unconstitutional general warrants. So, I think both of those cases are likely to continue to be litigated. And we'll see where things shake out at the end of the day.

If there's still a split, you know, something that the Supreme Court, I think, uh, would want to weigh in on.

Matt Adams: Yeah, for sure. We could probably talk about geofences all day, but in the interest of getting a good sampling of some of the hot-button issues that the NACDL Fourth Amendment Center is tracking and working through at this moment, let's move on to another issue: keyword searches. What exactly is the Fourth Amendment issue as it relates to keyword searches?

Michael Price: Oh, so this is another form of reverse warrant where the government, again, doesn't really have a suspect. So they go to Google and they say, hey Google, tell me everybody who searched for, say, the address where the crime occurred. And, uh, they get a list of every search and, you know, corresponding IP addresses and account info for people who ran that search. And from there, they'll try and identify a suspect.

So we've seen this come up in a bunch of contexts. And the most recent ended up in front of the Colorado Supreme Court in a case called the *People v. Seymour*. And the court there had some serious misgivings about the constitutionality of these types of warrants. The lack of probable cause and lack of particularity in their nature. But, ultimately ruled on good-faith grounds, which is ... We can have a conversation about the good-faith doctrine, the bane of my existence.

But, you know, these are reverse warrants, in the same way that the geofence warrant is reversed. But now we're talking about your search history. And, you know, once again, the argument here is that you have a privacy interest in your search history. The Colorado Supreme Court, in fact, found that. And if you have a privacy interest in it, then you're going to need a sufficient probable cause to go in and conduct this kind of search.

But here, you're searching through billions upon billions of Google users who are going about their daily lives typing, you know, fairly sensitive stuff into that, that box. People tend to treat it as almost a confessional sometimes, right?

Matt Adams: Yeah, what's this, what's this rash all about? Let me go to WebMD and figure it out.

I mean, there are some sensitive things that people put into their Google search history. But more than that, this general warrant issue is really front and center, because it's effectively allowing law enforcement to data-mine troves and troves and troves to just stumble across like, you know, how to dismember a body.

Whereas, in my version of the Fourth Amendment, I would think you'd need to have the suspect first, then articulate the probable cause as it relates, specific to that suspect, if they are accused of dismembering a body, and see if they were searching for how to dismember a body. But you can't, you can't let the tail wag the dog. And unfortunately, these technologies are just permitting that. Right?

Michael Price: Yeah, it's something that, you know, wasn't possible you know, too long ago was not something that Google did. And I should say that Google has, in fact, recognized that this is a problem. And, at least with with geofence warrants, they have stopped collecting that data. And instead of keeping it on their servers, keeping it directly on people's phones. Which will, at least going forward, ultimately, make it impossible for police to do these kinds of searches because the data won't be there. If you want to search everybody's location data, you're going to have to go search their individual phones to do it.

You know, but the fact that this, the technology is there, it's sort of like the "Field of Dreams" theory of privacy, right? If you build it, they will come. If you collect this data on millions of Americans, right, law enforcement is going to come knocking. Because they see it as a sort of, it's like hitting the easy button. I don't have to go and try and figure out who did it, you know, and get a warrant later. I can, I can just ask Google. And in fact, you know, about a quarter of all search warrants that Google is getting are these, these reverse type geofence and keyword warrants. That's about 40, 000 searches, or search warrants, every year.

Matt Adams: It's striking. It's scary. And it's a little bit Orwellian in the sense that we are really genuinely living through a time where technology is making our lives easier. It's allowing us to be places and do things that we never could imagine. But at the same time, it's really taxing these constitutional principles that we have fought so hard to protect. And it's really required legal ingenuity to try to take those historical principles that we hold dear and advance them at the pace of

technology. And damn is technology driving at a very, very quick speed at this point with the advent of technologies like artificial intelligence.

We've talked a lot about on this program about artificial intelligence. And I think it's probably most relevant in this concept of predictive policing. And on episode 42 of "The Presumption of Innocence," I talked with Pramod Kunju, who is the self-described AI guru. And he wrote the book, *Artificial Intelligence in Criminal Justice: A Primer on Implications, Ethics and Policy*. And I challenged him on this very issue. This notion that predictive policing is wrought with all kinds of issues if we don't put the effective guardrails around it when using AI.

I sat on the New Jersey Supreme Court's working committee on AI. And the first meeting, I was really struck by the fact that the court had really bought into AI, hook, line and sinker, as a valuable tool, in their view to criminal justice.

I want to get your take on that. Because I haven't seen, and I've said this publicly, a technology in my lifetime evolve at such a rapid pace as we've seen with AI.

Michael Price: Yeah, I think there's a real tendency to, sort of give too much weight to the technology here. And not understanding how this black box works, right?

In the defense world, we see AI in a bunch of different contexts. Predictive policing is one of them. You know, it comes up in facial recognition and forensic genetic genealogy.

Matt Adams: And we're going to talk about those, too, today.

Michael Price: It's all over the place. And, you know, there's a tendency to sort of rely on it without understanding how it works.

And, what we find every time we start to sort of look under the hood, is that it is far less reliable and accurate than you would think. And in large part, because it is, you know, based on sometimes historical data that is itself problematic. Right? So if you take your predictive policing example, and you feed it in all of the information about where there are recent arrests and think that's going to tell you, well, you know, I got to put more cops there, it becomes a self-fulfilling prophecy, right? They're going to arrest more people in that area. Send cops right back there. So you've got to really think about how these models work, what kind of data is going into them. And we don't have a lot of great information on that front. Often refer to as black-box technology, you know. You put something in, the machine does its work and out come the results. But how you get from A to B is sometimes the whole ballgame. And without any visibility into that process, it becomes a challenge from a defense perspective.

Matt Adams: To say nothing of the constitutional implications under *Brady* and its progeny about how it's actually working, because a lot of the companies developing this want to protect their intellectual property. And the governments that are buying this technology in some instances-- and I, I remember speaking with you, Mike, on a panel at the Inn of Court years ago, talking about the StingRay technology when, you know, that was the.... Unfortunately, technology's arriving at such a

pace right now that that almost seems like, you know, messenger pigeons at this point, compared to what we're talking about today. But there were agreements that these governments sign when they buy these technologies that say that if they're challenged to provide the way that their technology works, that they'll just dismiss the case and walk away because of the fact that they have invested... in a sense, I get it. They invested in developing the intellectual property. But that's squarely at odds with the *Brady* rights of a defendant who is entitled to understand exactly how that works.

Michael Price: Right. In a lot of these cases, whether you're dealing with a StingRay, or, uh, facial recognition, right, the game is often all about discovery at the beginning, and trying to get more information about the systems, the tools that were used and how they function.

And, you know, in the StingRay case, there were explicit instructions to drop cases should discovery be ordered. But there is a similar pattern going on now, say, with facial recognition. Every time we'd get a facial recognition case and file for discovery about the systems being used, if a court orders that discovery, it's not uncommon that you see the case, you know, that the government makes a plea offer that you can't refuse just to get the case to go away.

Matt Adams: Yeah, let's let's dig into that facial recognition as sort of another one of these technologies that our framers probably could never in their wildest dreams have imagined. But, I think it's really pronounced. I mean, before we got into recording this podcast, I walked into a Starbucks, bought a cup of coffee, used my cell phone to pay for it and it verified my identity by looking at my face. And I did that in a matter of 30 seconds. I paid for my coffee. I walked out and started talking to you. How is that playing out in the criminal justice world in terms of the Fourth Amendment issues that come to pass in this sort of Wild West of unregulated, untested and its sometimes flawed facial recognition technologies?

What's happening in the real world where that intersects with and collides with criminal justice?

Michael Price: Yeah, so one of the most important things to recognize is that the facial recognition that the cops are using is different than what you have on your cell phone in terms of face ID, right? That's a sort of one-to-one comparison. Your phone already knows what you look like. It's checking to see if it's you. Facial recognition is different because you are, you don't have a known individual here. You have an unknown and you're trying to identify somebody from a photo or video. And that means the identification is, first of all, only as good as the database underneath it and the training data for that software.

You may not be in that database, right? If the database is, say, made up of people's mugshots, and you haven't been arrested, you're not going to be in that database. But, the software will find somebody who looks very much like you. We call this a sort of doppelganger effect, where you can have the wrong person mistakenly identified.

And, once again, the process itself is pretty opaque in terms of the way each type of software identifies people, ranks candidates, you know, creates what it calls a match. And the reliability for these things has not been established. So that's where the Fourth Amendment issue comes in,

especially when, say, the probable cause for stopping somebody or arresting somebody is the facial recognition match, so to speak, and nothing more. Because then we say, well, how reliable was that, right? Didn't you just use a black-box algorithm to, you know, come up with what could be-- and is very likely --a highly suggestive identification procedure. You just had a machine find people that look very, very similar to this photo.

And now you have all of the regular sort of complications around eyewitness ID on top of that. So it's a tool that is widespread, but its reliability, again, just hasn't been established. And so that's something, uh, if you do get it in your case, obviously call us. But, you really want to be filing discovery motions, arguing *Brady*, trying to get at that reliability issue.

And New Jersey actually has a fantastic case, *Arteaga*, on this issue. So, facial recognition again, you know, very widespread, but you want to be challenging that reliability.

Matt Adams: How prevalent is facial recognition software out there? And I mean, in the context of not me buying my cup of coffee, but I mean, you know, how prevalent are these cameras that we see everywhere now?

How prevalent are they linked to facial recognition? How frequently is that happening? Places where people congregate, stadiums, is that basically widespread at this point?

Michael Price: So, I would say the, well, the earliest system started in around 2001. By 2016, about a quarter of all law enforcement agencies had facial recognition technology. Most of that is used for investigative purposes based on, you know, sort of, surveillance photos or video. But it's generally not in real time.

I think one of the things that we've seen in the news recently has been, as you say, large stadiums using facial recognition in real time to identify people at the stadium, right? Casinos do it as well. So that technology definitely exists and mostly in the private sector at the moment.

But I think the great fear, the privacy fear here, is a world in which you've got facial recognition running in real time on, you know, the city's network of closed-circuit cameras or body cams on police officers. We are not there yet, but that is, you know, that that is one dystopia that I don't want to live in.

Matt Adams: Wow. We're talking with Mike Price. An eye-opening exploration of the intersectionality between these advanced technologies that we're dealing with in our society and the Fourth Amendment.

He's with the NACDL's Fourth Amendment Center, true expert in the field.

Let's go to another one of these technologies, Mike, and that is forensic genetic genealogy. We have a society that has been convinced it's necessary for them to swab their mouth, send it into a lab -- they don't know where they're sending it to-- and, wait a couple of weeks and get a profile of their genealogy, and then go online and try to find their long-lost cousins. But there's some hidden

danger in that isn't there? Because once you avail yourself of that exercise, you have basically released your genetic profile, having it be subject to potential examination. Right?

Michael Price: Yeah, so this is, uh, this is another one of those, you know, sort of reverse type of search. But this time, you are dealing with genetic and familial relationships between people. So what'll happen here? You see this a lot and in cold cases, where the police have a DNA sample from a suspect who's unknown. And they don't get any hits in CODIS.

And so, the new tool here is to take that DNA, do some editing to it, because generally it's pretty degraded. So there's a little bit of black-box magic that goes on there. And, uh, and you have a company or law enforcement who will take that and put it into a service like Family Tree DNA or 23andme and use it to identify common ancestors of that individual. And then they sort of build out a family tree from there and identify a list of potential suspects for the police to go and investigate. The company that we see most frequently doing this is a company called Parabon NanoLabs.

So, if you see that in one of your cases, definitely want to give us a call. But, you know, again, it's tempting to view this as science. And there's some science involved, but it is also, you know, a real black box in terms of how that process works, of identifying family members and building out a tree. It's a lot of Googling, frankly, right? And genealogical research that goes into this. It's not straight DNA. You know, it starts with DNA and then sort of goes off a cliff from there. So this is, it's a very new type of technology and one, again, whose reliability has not been established. So, you know, we're seeing arrest warrants and search warrants based off of a forensic genetic genealogy hit or report. And how reliable that report or that hit may be is a real open question. Even the company that does it says it shouldn't be used for probable cause. And yet we see that happening all the time.

Matt Adams: And let me get this straight. So a DNA sample is collected, perhaps at a crime scene.

Okay. It's taken into custody and analyzed, collected and analyzed by law enforcement. A genetic profile is developed through some sort of black-box technology that oftentimes we can't get discovery about. That profile is then shared with one of these commercially available repositories of this genetic information and they ask if it matches anything that's in their systems?

Michael Price: Yeah, oftentimes you're not looking for a straight match. What they will do is they'll find common genetic ancestors and then build out a family tree from there. So they'll say, well, this person must be related to these other people, and sort of build out the tree from there. That is, part of this process that, again, I think, you know, hasn't been established as a reliable method of identification. But that is certainly what they're trying to do.

Matt Adams: Wow. As if that wasn't enough, um, let's get out of the sci-fi world and go

back to what seems like an archaic technology, which is something you and I've worked on together, which is the idea of mobile device seizure, and some of the issues that arise under the Fourth Amendment there. Because I'm still struck by the fact that these devices we carry around in our pockets today, and I think the Supreme Court, to its infinite credit, --and I don't necessarily agree with a lot of what the Supreme Court is doing lately-- but when it comes to mobile technology with

cases like *Carpenter*, they seem to get it. They seem to get exactly the Pandora's box that this little brick that we carry in our pockets, and we're frankly addicted to and can't go anywhere without, they seem to understand how much stuff it really contains.

And what strikes me, though, is that once there's articulated probable cause to get into this thing, the cases that I've seen suggest that everything is fair game. And to me, the particularity requirements that the Fourth Amendment has would really be contrary to that notion. And that law enforcement really should be able to say, I want to look at Mike Price's photos, and here's the reason why. Here's my probable cause why.

But that doesn't give access to Mike Price's email or bank records or medical records, all of which are now contained on these devices. So we went from a device that was relatively dumb by today's standards to these devices that can do just about everything, including buy a cup of coffee, in my other example previously.

I mean, where does it stop? And is there any movement to get courts to force a more specific particularity requirement about which portion of the phone should be searched or seized?

Michael Price: Yeah, I mean, device searches are so prevalent now, right?

We all --

Matt Adams: Every case I have at this point has a mobile device collection issue. To say nothing of the other collections, like emails and things like that. I don't have a case that I'm handling right now where a mobile device is not involved.

Michael Price: Yeah, I mean, this used to be something of a niche issue and now it is, almost every case has a device search issue. And the law has really been stuck for a little while, right? It used to be that the police would say, establish probable cause to search the phone, right? But at the time, the Supreme Court was deciding *Riley*. You know, we're still talking about a flip phone, you know, with a green screen and some contacts in there, maybe.

Matt Adams: I don't know if you remember this, Mike, but at the oral argument on *Andrews* at the New Jersey Supreme Court, I had to borrow somebody's old flip phone. And I pulled it out of my pocket. Now, some of the justices were amused and some were not. But I literally pulled it out of my pocket and I said, We're not dealing with this anymore, right? We're dealing with something more, more unique, more nooks and crannies, more compartments. You know, it's the whole automobile search thing going all over again. That law school examples of, can you search the locked glove compartment of the trunk? What's your probable cause? We're back there. And for the life of me, they don't seem to get it.

Michael Price: Yeah. I think we're now reaching the point where we're having more of these wins on device search cases, because judges are starting to get it, and recognizing just how much information is on a single cell phone. It, you know, may contain more private information that you

would have in your house. And probably, you know, information that doesn't even exist in your house, like your location data, right?

And so, when you're talking about probable cause, it's probable cause for what? What data on the phone can you search? If you have probable cause for location data, great. And there should be a date restriction on that as well. Um, if you're looking for messages again, you want to be, you know, arguing for some sort of particularization relative to the probable cause that you have.

And beware of these sort of catch-all phrases in warrants, too. A lot of times you'll see, as a case that's going to be going before the 9th Circuit dealing with the question of, you know, can you search everything on the phone just for evidence of user attribution, right?

So, we have a warrant that was actually fairly specific, right? Said you can search for videos between this date and this date. But then had a clause in there that said, well, you can search anything else on the computer just for purposes of identifying user attribution, right?

Matt Adams: That's bonkers. That is bonkers.

Michael Price: And so, it turns what would otherwise be a limited search into a general search. And everything then becomes in plain view and nothing is off limits.

So, you know, our argument there is, that sort of warrant, you know, lacks probable cause, lacks particularization, for data outside of that limited timeframe.

And so like, I said, we are getting some somewhere on this. There's been a series of decisions in New York recently related to cell phone searches and finding that, say an officer's training and experience, is insufficient to justify a cell phone search without some sort of nexus between the phone and the crime.

You can't just say, Well, in my training and experience, criminals have phones and it's got evidence on them, right? It doesn't cut it. You have to say, what, why do you think there's evidence on that particular phone? And what evidence do you think you're going to find?

You can't just say, well, phones, evidence. And you had a couple of decisions, recognizing that cell phone searches at the border have to be conducted with a warrant. So this has been one of those loopholes for a while, the border search exception. And you would see people getting searched without a warrant, either coming in or even leaving, when they leave the country. It's like, you know, the police don't have probable cause to search your phone, but they know that you're getting on an airplane tomorrow. And so, seize your phone at the border as you're leaving the country. And, that was *U.S. v. Shapiro* finding that the border search exception does not apply for a phone when you're leaving the country. And then there was a *U.S. v. Sultanov* holding that a warrant is required for even a manual ordered search of a cell phone.

So I think we are making some headway here, but, you know, it's slow going and I think defense counsel need to be raising these issues in their cases. And we're more than happy to help you do that.

Matt Adams: Yeah, it's almost like the government wants us to read out the following from the Fourth Amendment, "and particularly describing the place to be searched and the persons or things to be seized."

They don't issue warrants to go and search an entire apartment building. They give a warrant for a particular unit or units within that apartment building. And I think the phone is no different when it comes to these particularity issues.

And where I want to end today is on the issue where we first met, which is compelled decryption. And a lot of these issues come to light because of compelled decryption and the wacky Wild West of case law that's developed around this issue that desperately needs to be resolved by the Supreme Court once and for all. Because we've got this sort of patchwork of cases that really don't make a lot of sense if you're a proponent of the Fourth Amendment, one in New Jersey in particular that I was involved in. But when it comes to compelled decryption-- and that is a police officer, or a law enforcement agent forcing you to unlock your phone to make it easier to perform that generalized search that we just got done talking about-- what's the state of play right now with respect to that?

Michael Price: Yeah, so this is an issue. If you have a cell phone in your case, and you have a cell phone search in your case, you always want to be asking the question: How did they get into the phone? You know, the government does have some tools that allow them to sort of crack and hack their way into a phone.

But sometimes, it'll be the officer saying, No, no, no. Just tell me your passcode. Come on, let's, you know, open up your phone. Or you'll have a warrant requiring somebody to unlock their phone. And then the question becomes, is that constitutional, right? What about your Fifth Amendment rights?

And, the law right now is sort of all over the place, as you alluded to earlier. Some courts will look at this and say, Well, you know, it's, just like providing the key to your safe deposit box.

Matt Adams: It's not!

Michael Price: You know, there's no difference and, the--

Matt Adams: It's a password, and my response during our oral argument was, what if my password is "I just killed somebody."

Michael Price: No, I, think you have other courts that do recognize it is not like producing a physical key, that it involves compelling you to, you know, utilize your mind, right? And reveal the secret passcode. So in that sense, it's testimonial, right? It is not just like handing over the key.

And so the courts have actually split on that issue. And then there's the additional question of whether they can force you to open it using your fingerprint or your face ID. And, you know, well, that doesn't require you to say anything, right? It doesn't require you to produce the contents of your mind.

But, it is effectively doing the same thing, right? And you can't have a face ID without a passcode set up on the phone. And since there's no functional difference between the two, you know, how does that land, for Fifth Amendment purposes? And the courts, once again, are split on that issue. Some of them saying, Yeah, it's okay to, it's not compelled decryption if it's a face ID, and some saying yes, it is.

So, it is, the law right now is very much all over the place. I do think that this is an issue that the Supreme Court is eventually going to have to weigh in on. I don't know when that's going to happen, but it's an incredibly important issue. And it's, increasingly prevalent. Again, if you have a cell phone search in the case, you want to be asking, how did the police get it? Did they compel your client to give that passcode? If so, you may have a Fifth Amendment argument there.

Matt Adams: Well, Mike, what we're talking about, I think, can easily keep us busy for the next decade or so. But I think there's going to be a host of additional issues that start to come to light that may make these look like that passenger pigeon I talked about earlier, where we're laughing about how primitive these technologies seem.

What keeps you up at night? What keeps you as the litigation director at the Fourth Amendment Law Center of the NACDL up at night about what's on the horizon at the intersection of the law and technology?

Michael Price: Yeah, I mean, I think the scary part to me is that most of the tech that we're dealing with now has been around for a little while, and it has taken a number of years for it to be disclosed, for defense lawyers to recognize it and for it to be challenged and put in front of courts, right?

Geofence warrants, started, you know, before 2016. You know, we still don't have a definitive answer on their constitutionality. The cases are just now making their way up to the courts of appeals. And so I think what is scary is how far behind the law is lagging. We may, you know, get a good law on a device search case or a geofence case, but the next thing will have already been going on, and, you know, I think until the law catches up, we're sort of going to be playing whack-a-mole with these Fourth Amendment issues. That by the time a court gets their hands on it and reaches a decision, we're already off dealing with the next technology.

And so, you know, it's that pace of the developmental law that really bothers me. I don't have any more scary new tech to tell you about. I think it's the tech that we don't know about yet that worries me. And, that's why, you know, part of the reason the Fourth Amendment Center exists is to identify these things and help defense lawyers bring these challenges when it might be otherwise hard to just do on your own. They're big, they're complex issues. But they are important ones. And if we are going to get the law to catch up, we have to start recognizing them and litigating them in our cases.

Matt Adams: Well, amen to that, Mike. What we've been talking about for the better part of the last hour is a bit of a Orwellian existence in today's society. We can't get away from technology. We've embraced it, hook, line and sinker. But the issues it creates are enormous and impactful and touch on the most fundamental rights that we hold dear as Americans. You know, in *1984*, the Orwellian book that, I'm struck, there's a quote: "If you want to keep a secret, you must also hide it from yourself."

Are we ever going to go back to a place where there is true privacy?

Michael Price: You know, I don't think that we need to shun technology. I like technology. Makes my life easier. I do like privacy, and I don't think that privacy has to die with new technology, but I do think that we need to understand that technology, and you know, put those guardrails in place now. It can be very tempting to go and try and hit the easy button and ask Google who did it. And if we don't put the brakes on that now and establish those guardrails, I do fear, you know, what the next decade will look like. But I think we have an opportunity here to try and rein it in and craft some semblance of privacy.

Matt Adams: Well, Mike, thanks so much for joining us on "The Presumption of Innocence." Mike Price from the NACDL Fourth Amendment Center. It has been a thought-provoking hour or so with you. Until next time. We'll see you on "The Presumption of Innocence." I'm Matt Adams. Take care.